M2047-5
T. KATSURA
H. INOUE
#2

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed h this Office.

出願年月日
Date of Application: １９９９年　９月２２日

出願番号
Application Number: 平成１１年特許願第２６８８２８号

出願人
Applicant (s): 松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年　６月２３日

特許庁長官
Commissioner,
Patent Office
近藤隆彦

出証番号　出証特２０００－３０４６７８２

【書類名】　特許願

【整理番号】　2038610019

【提出日】　平成11年 9月22日

【あて先】　特許庁長官殿

【国際特許分類】　G09F 19/00

G09C 5/00

H04N 1/387

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　桂　卓史

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　井上　尚

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097179

【弁理士】

【氏名又は名称】　平野　一幸

【手数料の表示】

【予納台帳番号】　058698

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　電子署名装置、電子署名方法及びそのプログラムを記録した記録媒体

【特許請求の範囲】

【請求項１】電子的に表示される用紙に署名画像を貼り付ける電子署名装置であって、

生の署名画像を入力する署名画像入力部と、入力された生の署名画像に電子透かしを埋め込む透かし埋め込み部と、電子透かしが埋め込まれた署名画像を蓄積する埋め込み済み画像記録部とを備え、

前記透かし埋め込み部は、用紙毎にユニークな付加情報を、署名画像に埋め込むことを特徴とする電子署名装置。

【請求項２】前記透かし埋め込み部は、用紙毎にユニークな付加情報を、署名画像の輪郭付近に集中して埋め込むことを特徴とする請求項１記載の電子署名装置。

【請求項３】前記画像記録部は、電子透かしが埋め込まれた署名画像を含む、用紙全体の画像を蓄積することを特徴とする請求項１または２記載の電子署名装置。

【請求項４】電子的に表示される用紙に署名画像を貼り付ける電子署名装置であって、

生の署名画像を入力する署名画像入力部と、入力された生の署名画像に電子透かしを埋め込む透かし埋め込み部とを備え、

前記透かし埋め込み部は、生の署名画像由来の画像を二次元ウェーブレット変換し、その変換係数のうち、零の値を持つ変換係数はそのままにし、非零の値を持つ変換係数に対して、用紙毎にユニークな付加情報を反映した処理を施して電子透かしを埋め込み、さらに変換係数を逆二次元ウェーブレット変換して、電子透かしが埋め込まれた署名画像を生成することを特徴とする電子署名装置。

【請求項５】前記生の署名画像由来の画像は、生の署名画像の振幅値を定数倍したものであることを特徴とする請求項４記載の電子署名装置。

【請求項６】前記付加情報は、用紙毎にユニークに付与される識別子を含む情

報をビット展開したビット列であることを特徴とする請求項１又は４記載の電子署名装置。

【請求項７】電子透かしが埋め込まれた署名画像から、用紙毎にユニークな付加情報を取り出す透かし取り出し部を有することを特徴とする請求項１又は４記載の電子署名装置。

【請求項８】用紙に貼り付けられる署名画像を参照し、この署名画像が生の署名画像でなく、かつ、この署名画像から前記透かし取り出し部が取り出した付加情報が正当でないとき、不正判断を行い、署名を拒否する制御部を有することを特徴とする請求項７記載の電子署名装置。

【請求項９】前記署名画像は、捺印、サイン又は指紋のいずれかの画像であることを特徴とする請求項１から８記載の電子署名装置。

【請求項１０】電子的に表示される用紙に署名画像を貼り付ける電子署名方法であって、

生の署名画像に電子透かしを埋め込む透かし埋め込みステップと、電子透かしが埋め込まれた署名画像を蓄積する埋め込み済み画像記録ステップとを備え、

前記透かし埋め込みステップでは、用紙毎にユニークな付加情報を、署名画像に埋め込むことを特徴とする電子署名方法。

【請求項１１】前記透かし埋め込みステップでは、用紙毎にユニークな付加情報を、署名画像の輪郭付近に集中して埋め込むことを特徴とする請求項１０記載の電子署名方法。

【請求項１２】前記画像記録ステップは、電子透かしが埋め込まれた署名画像を含む、用紙全体の画像を蓄積することを特徴とする請求項１０記載の電子署名方法。

【請求項１３】電子的に表示される用紙に署名画像を貼り付ける電子署名方法であって、

生の署名画像に電子透かしを埋め込む透かし埋め込みステップとを備え、

前記透かし埋め込みステップでは、生の署名画像由来の画像を二次元ウェーブレット変換し、その変換係数のうち、零の値を持つ変換係数はそのままにし、非零の値を持つ変換係数に対して、用紙毎にユニークな付加情報を反映した処理を

施して電子透かしを埋め込み、さらに変換係数を逆二次元ウェーブレット変換して、電子透かしが埋め込まれた署名画像を生成することを特徴とする電子署名方法。

【請求項１４】前記生の署名画像由来の画像は、生の署名画像の振幅値を定数倍したものであることを特徴とする請求項１３記載の電子署名方法。

【請求項１５】前記付加情報は、用紙毎にユニークに付与される識別子を含む情報をビット展開したビット列であることを特徴とする請求項１０又は１３記載の電子署名方法。

【請求項１６】電子透かしが埋め込まれた署名画像から、用紙毎にユニークな付加情報を取り出す透かし取り出しステップを有することを特徴とする請求項１０又は１３記載の電子署名方法。

【請求項１７】用紙に貼り付けられる署名画像を参照し、この署名画像が生の署名画像でなく、かつ、この署名画像から前記透かし取り出しステップが取り出した付加情報が正当でないとき、不正判断を行い、署名を拒否することを特徴とする請求項１６記載の電子署名方法。

【請求項１８】前記署名画像は、捺印、サイン又は指紋のいずれかの画像であることを特徴とする請求項１０から１７記載の電子署名方法。

【請求項１９】生の署名画像に電子透かしを埋め込む透かし埋め込みステップと、電子透かしが埋め込まれた署名画像を蓄積する埋め込み済み画像記録ステップとを備え、

前記透かし埋め込みステップでは、用紙毎にユニークな付加情報を、署名画像に埋め込むことを特徴とする電子署名プログラムを記録した記録媒体。

【請求項２０】前記透かし埋め込みステップでは、用紙毎にユニークな付加情報を、署名画像の輪郭付近に集中して埋め込むことを特徴とする請求項１９記載の電子署名プログラムを記録した記録媒体。

【請求項２１】前記画像記録ステップは、電子透かしが埋め込まれた署名画像を含む、用紙全体の画像を蓄積することを特徴とする請求項１９記載の電子署名プログラムを記録した記録媒体。

【請求項２２】生の署名画像に電子透かしを埋め込む透かし埋め込みステップ

とを備え、

前記透かし埋め込みステップでは、生の署名画像由来の画像を二次元ウェーブレット変換し、その変換係数のうち、零の値を持つ変換係数はそのままにし、非零の値を持つ変換係数に対して、用紙毎にユニークな付加情報を反映した処理を施して電子透かしを埋め込み、さらに変換係数を逆二次元ウェーブレット変換して、電子透かしが埋め込まれた署名画像を生成することを特徴とする電子署名プログラムを記録した記録媒体。

【請求項２３】前記生の署名画像由来の画像は、生の署名画像の振幅値を定数倍したものであることを特徴とする請求項２２記載の電子署名プログラムを記録した記録媒体。

【請求項２４】前記付加情報は、用紙毎にユニークに付与される識別子を含む情報をビット展開したビット列であることを特徴とする請求項１９又は２２記載の電子署名プログラムを記録した記録媒体。

【請求項２５】電子透かしが埋め込まれた署名画像から、用紙毎にユニークな付加情報を取り出す透かし取り出しステップを有することを特徴とする請求項１９又は２２記載の電子署名プログラムを記録した記録媒体。

【請求項２６】用紙に貼り付けられる署名画像を参照し、この署名画像が生の署名画像でなく、かつ、この署名画像から前記透かし取り出しステップが取り出した付加情報が正当でないとき、不正判断を行い、署名を拒否することを特徴とする請求項２６記載の電子署名プログラムを記録した記録媒体。

【請求項２７】前記署名画像は、捺印、サイン又は指紋のいずれかの画像であることを特徴とする請求項１９から２６記載の電子署名プログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、紙の用紙に、押す又は書き込んで、署名していた環境に似た環境を、電子的に実現する電子署名装置及びその関連技術に関するものである。ここで、本明細書にいう「署名」とは、一般の概念より広義であって、署名者が用紙に

記載された事項を認めるあかしとして行う行為又はこの行為の結果生ずる画像をいい、捺印、サイン、指紋を付すことなどを総称する。

【０００２】

【従来の技術】

近年、オフィスでは、電子化、ペーパーレス化が進み、書類を紙に出力せず、モニターに表示するだけで、処理することが増えている。この際に問題となってくるのが、署名の取り扱いである。

【０００３】

ここで、紙を用いた署名では、用紙に付された署名を、目視などで検査していた。また、用紙に付された署名を、悪意をもって、他の署名に転用することは、非常に難しい。

【０００４】

しかしながら、ペーパーレスの環境下において、署名画像の情報を単にデジタル化して電子文書に貼り付けたのでは、署名画像データはデジタルであり、完全な複製を作ることができるので、署名画像データを勝手に複製し、他の文書に貼り付けるような、不正行為を簡単に行うことができる。

【０００５】

このような不正行為の防止策として、「インターネットセキュリティ：佐々木良一他共著（オーム社）」１２０ページに、電子捺印（ｄｉｇｉｔａｌ　ｓｉｇｎａｔｕｒｅ）に関し、次のような記述がある。

【０００６】

即ち、用紙データをハッシュ関数に入力し、ハッシュ値に変換する。なお、１つのハッシュ値に対して世の中には１つの用紙しか存在しないという関係がある。そして、このハッシュ値に属性情報（電子捺印の種類を示す記号、時間情報）を結合させる。属性情報が結合されたハッシュ値を、公開鍵暗号（署名検査者の秘密鍵を使用）により変換する。この変換結果を、電子捺印とし、電子捺印付きの用紙データを次の署名検査者に送信する。この電子捺印は、秘密鍵の持ち主（この場合署名検査者）しか作成できない。

【０００７】

電子捺印の検証においては、送られてきた電子捺印を送信者の公開鍵暗号により変換する。送信側での処理がすべて正しく行われたとすると、公開鍵暗号による変換結果は、送信側で生成された属性情報が結合されたハッシュ値と等しくなる。そこで、送られてきた用紙データをハッシュ関数に入力して得られたハッシュ値と、公開鍵暗号による変換結果とを比較し、ハッシュ値が一致すれば認証となる。

【０００８】

【発明が解決しようとする課題】

しかしながら、上記電子捺印の技術では、署名を目視により検査する、従来の慣習から、あまりにも、かけ離れており、これに接する一般人は、違和感を禁じ得ない。

【０００９】

また、電子捺印の技術は、電子取引を想定して構築されたものであり、一対一の場合には適している。しかし、用紙には、複数の署名者がそれぞれ署名を行うことも多く、これに対応するには、複数の公開鍵暗号を用意する必要があり、実用に供し難い。

【００１０】

さて近年、電子透かしによって、特定のセキュリティデータを画像に埋め込む技術が実用化されているので、これを利用することも考えられる。ここで、署名の性質として、次のような点をあげることができる。

（性質１）署名は、単色（通常、白）の地に単色（赤、黒、青など）で書されてなる。したがって、少なくとも輝度レベルで見ると、２値画像そのものか、それに非常に近い。

（性質２）署名の画像は、様々な用紙に繰り返し同じものが使用され、さらに同一の用紙の複数箇所に同一の署名の画像が使用されることがある。

【００１１】

しかしながら、従来の電子透かしは、画像全体に目立ちにくい誤差を分散させるものばかりであり、署名の性質に合わせて特化されていない。

【００１２】

即ち、従来の電子透かしによると、性質１に対して、２値画像の全体に電子透かしが分散することになり、透かしが目立ちやすく、紙の用紙に署名を行った場合に比べると、見た目がかなり変わって、不自然になりやすい。

【００１３】

また、性質２に対し、従来の電子透かしは、用紙と関係なしに、しかも、画像に依存して埋め込まれるので、同じ画像を繰り返し使用する、署名の画像では、複数の署名の画像に、同じ電子透かしが埋め込まれる可能性があり、セキュリティ上問題になりやすい。本来、従来の電子透かしは、著作権情報や商標など、用紙と全く無関係（用紙が変わっても不変）の情報を埋め込むようになっているから、このようなことになり、署名の画像には不適当なのである。

【００１４】

そこで本発明は、従来の慣習に近く、かつ署名の性質に合った電子署名装置及びその関連技術を提供することを目的とする。

【００１５】

【課題を解決するための手段】

本発明では、署名画像入力部から生の署名画像を入力し、入力された生の署名画像に、透かし埋め込み部が電子透かしを埋め込み、埋め込み済み画像記録部に電子透かしが埋め込まれた署名画像を蓄積するものであり、この透かし埋め込み部は、用紙毎にユニークな付加情報を、署名画像に埋め込むこととした。

【００１６】

これにより、従来の慣習に近く、かつ署名の性質に合った電子署名装置を実現できる。

【００１７】

【発明の実施の形態】

請求項１記載の発明では、生の署名画像を入力する署名画像入力部と、入力された生の署名画像に電子透かしを埋め込む透かし埋め込み部と、電子透かしが埋め込まれた署名画像を蓄積する埋め込み済み画像記録部とを備え、透かし埋め込み部は、用紙毎にユニークな付加情報を、署名画像に埋め込む。

【００１８】

この構成により、生の署名画像に、電子透かしが埋め込まれ、埋め込み済み画像記録部に蓄積される。そして、埋め込まれる電子透かしは、用紙毎にユニークに付与される付加情報である。したがって、ある用紙において使用された、電子透かし埋め込み済みの署名画像を、悪意をもって他に転用しようとしても、その署名画像は、その用紙固有のものであるから、すぐに不正が露呈する。このため、同様の画像が繰り返し使用される、署名画像において、不正転用を牽制して、十分なセキュリティを確保できる。

【００１９】

請求項２記載の発明では、透かし埋め込み部は、用紙毎にユニークな付加情報を、署名画像の輪郭付近に集中して埋め込む。

【００２０】

この構成によって、電子透かしは、署名画像の全体に分散して埋め込まれるのではなく、署名画像の輪郭付近に集中して、局所的に埋め込まれる。ここで、２値画像又はそれに近い低階調の画像では、輪郭付近の変化が知覚されにくい。したがって、一般的に透かしが目立ちやすい、署名画像においても、それとわからない電子透かしを埋め込むことができ、紙の用紙に直接署名していた、従前の慣習に近く、違和感が少ない、言い換えれば、署名の性質に特化した、環境を実現できる。

【００２１】

請求項３記載の発明では、画像記録部は、電子透かしが埋め込まれた署名画像を含む、用紙全体の画像を蓄積する。

【００２２】

この構成により、透かし埋め込み済みの署名画像だけでなく、用紙にこれを貼り付けた画像として、蓄積するため、用紙全体のイメージを即座に、しかも簡単に取り出すことができる。また、取り出した用紙全体のイメージに含まれる署名画像を部分的に切り出して転用しようとしても、請求項１同様のセキュリティがあるため、このような不正を抑制できる。

【００２３】

請求項４記載の発明では、生の署名画像を入力する署名画像入力部と、入力さ

れた生の署名画像に電子透かしを埋め込む透かし埋め込み部とを備え、透かし埋め込み部は、生の署名画像由来の画像を二次元ウェーブレット変換し、その変換係数のうち、零の値を持つ変換係数はそのままにし、非零の値を持つ変換係数に対して、用紙毎にユニークな付加情報を反映した処理を施して電子透かしを埋め込み、さらに変換係数を逆二次元ウェーブレット変換して、電子透かしが埋め込まれた署名画像を生成する。

【００２４】

この構成において、二次元ウェーブレット変換し、その変換係数のうち、零の値を持つ変換係数はそのままにし、非零の値を持つ変換係数に対して、用紙毎にユニークな付加情報を反映した処理を施して電子透かしを埋め込むので、署名画像の輪郭付近に電子透かしが集中して埋め込まれる。このため、請求項２同様の作用効果が得られるだけでなく、周波数成分により分割される各領域に対応した電子透かしを埋め込める。即ち、一又は二以上の特定の領域にのみ、電子透かしを埋め込むようにすれば、この特定の領域のみをアクセスすることで、電子透かしの抽出を、より容易にすることができる。

【００２５】

請求項５記載の発明では、生の署名画像由来の画像は、生の署名画像の振幅値を定数倍したものである。

【００２６】

この構成により、２値画像又はそれに近い低階調の署名画像に対し、より知覚されにくい電子透かしを埋め込むことができる。

【００２７】

請求項６記載の発明では、付加情報は、用紙毎にユニークに付与される識別子を含む情報をビット展開したビット列である。

【００２８】

この構成により、小さく、軽い情報の埋め込みを行うだけで、十分なセキュリティを確保でき、かつ、演算処理負担を軽減して、処理時間を短縮することができる。しかも、生の署名画像と埋め込み画像済み署名画像との見た目の差を極力少なくすることができる。

【００２９】

請求項７記載の発明では、電子透かしが埋め込まれた署名画像から、用紙毎にユニークな付加情報を取り出す透かし取り出し部を有する。

【００３０】

この構成により、取り出した付加情報を利用して、不正の抑制に資することができる。

【００３１】

請求項８記載の発明では、用紙に貼り付けられる署名画像を参照し、この署名画像が生の署名画像でなく、かつ、この署名画像から透かし取り出し部が取り出した付加情報が正当でないとき、不正判断を行い、署名を拒否する制御部を有する。

【００３２】

この構成における、制御部により、目で見ただけでは判別困難な不正を、正確かつ高速に知ることができ、不正署名をシステム上で排除できる。

【００３３】

請求項９記載の発明では、署名画像は、捺印、サイン又は指紋のいずれかの画像である。

【００３４】

この構成により、現場で使用される署名画像の全てに対応できるし、一部分には捺印が使用され、他の部分にはサインが使用されるような、複数種の署名画像が混在して使用される場合にも対応できる。

【００３５】

次に、図面を参照しながら、本発明の実施の形態を説明する。図１は、本発明の一実施の形態における電子署名装置のブロック図である。図１に示すように、この電子署名装置は、次の構成要素を有する。まず、制御部１は、ＣＰＵ（中央処理装置）及びそれに参照されるＲＡＭ（ランダムアクセスメモリ）などからなり、電子署名装置の他の要素の動作を制御すると共に、図５のフローチャートに沿って、署名の正／不正判断を行い、不正と判断するときは、署名を拒否する。なお、その詳細は、後述する。

【００３６】

表示部２は、ＬＣＤやＣＲＴ等からなり、署名者に、用紙、署名画像など、必要な情報を表示する。入力部３は、キーボードやマウスなどからなり、署名者がログインＩＤを入力したり、その他必要な指示を与えるためのものである。

【００３７】

署名画像入力部４は、スキャナなどからなり、署名者や管理者は、これを用いて、生の署名画像を入力する。署名画像データベース５は、記憶装置及びこれに対して読み書きを行うデータベースエンジンからなり、入力された生の署名画像（電子透かし埋め込み前）を蓄積する。なお、署名画像データベース５に蓄積される、生の署名画像は、生の署名画像そのものであっても良いし、当該署名画像に係る署名権者のＩＤ等を電子透かしとして埋め込んだものでも良い。本明細書において、署名画像データベース５に蓄積される署名画像を、生の署名画像という。

【００３８】

用紙マスタデータベース６は、署名画像が貼り付けられていない、用紙（様式）の情報を蓄積する。用紙の情報は、表示部２に用紙の画像を表示（再現）できれば、その形式は任意であって、ラスタ系またはベクタ系の画像情報であっても良いし、ＨＴＭＬファイルのようにテキスト系の情報であっても良いが、通常、ファイルやファイルの一部のフィールドとして保存される。

【００３９】

埋め込み情報付与部７は、用紙マスタデータベース６から作成される用紙に対して、用紙毎にユニークな付加情報を付与する。この付加情報は、用紙毎にユニークに付与される識別子を含む。こので、「用紙毎にユニーク」とは、様式が同じであっても、用紙そのものが異なれば、別個であるという意味である。単純な例を挙げると、様式１と様式２の二種類の様式が存在し、様式１に従う用紙が、用紙Ａ、用紙Ｂの２枚あり、様式２に従う用紙が、用紙Ｃ、用紙Ｄ、用紙Ｅの３枚あったとすると、用紙Ａ～用紙Ｅの全てについて、互いに重複することのない、識別子が付与されることになる。このような関係を採用することによって、様式が同じ用紙間においても、署名画像の不正転用を防止できる。

【００４０】

さらに、この付加情報には、他の任意の情報を追加しても良い。追加する情報としては、用紙が作成された時刻の情報や、署名者のＩＤ、用紙の様式情報などが考えられる。但し、追加する他の情報は、必要最小限にして、取り扱う情報量を小さくした方が、処理速度の点で有利であり、好ましい。

【００４１】

そして、本形態では、この付加情報は、埋め込み情報付与部７によって、ビット展開され、ビット列（各ビットは、「０」か「１」）として、利用される。但し、埋め込み情報付与部７は、この付加情報を付与するだけにして、他の要素（例えば制御部１）において、ビット展開するようにしても良い。

【００４２】

透かし埋め込み部８は、署名画像データベース５から、生の署名画像を入力すると共に、上記のように、ビット展開されたビット列を入力する。そして、図２のフローチャートに沿って、生の署名画像に電子透かしを埋め込み、埋め込み済み署名画像を得て、これを出力する。また、この埋め込みは、後に詳述するように、署名画像の輪郭付近に集中する。

【００４３】

透かし取り出し部１０は、埋め込み済み用紙データベース９に蓄積された画像から、制御部１が取り出した、埋め込み済み署名画像を入力する。そして、図４に示すフローチャートに沿って、埋め込み済み署名画像から、埋め込みビット列を取り出すと共に、埋め込み前の生の署名画像を再生し、これらビット列と生の署名画像とを出力する。

【００４４】

次に、図２を用いて、透かし埋め込み部８の動作を説明する。ここで、本形態では、図３に示すような、離散ウェーブレット変換による変換係数ＬＬ、ＨＬ、ＬＨ、ＨＨを用いる。図では、簡単のため、１階層のウェーブレット変換による変換係数を示しているが、２、３、またはそれ以上の階層としても良い。さらには、ウェーブレット変換ではなく、サブバンド分割による変換係数を用いても差し支えない。

【００４５】

さて、図２に示すように、ステップ１にて、透かし埋め込み部８は、署名画像データベース５から生の署名画像を入力する。この署名画像には、発明の属する技術分野の項で述べたように、捺印、サイン、指紋などのいずれでも良く、階調や色なども任意である。但し、現実には、発明が解決しようとする課題の項において、（性質１）として指摘したように、署名画像は、ほとんど２値画像であるといっても良い。

【００４６】

次に、ステップ２にて、透かし埋め込み部８は、埋め込み情報付与部７から埋め込みビット列を取得する。なお、ステップ１、２の順序は、逆にしても良い。

【００４７】

ステップ３では、透かし埋め込み部８は、入力した生の署名画像に対し、その全画素の振幅値をα（１より大きい整数）倍する。このようにすることにより、２値画像またはそれに近い、署名画像のダイナミックレンジを広くして、つまり、階調を意図的に大きくして、埋め込まれる電子透かしを、より知覚されにくくすることができる。

【００４８】

次に、透かし埋め込み部８は、ステップ４にて、振幅値をα倍した署名画像を、二次元ウェーブレット変換し、変換係数ＨＬ、ＬＨ、ＨＨを取得する（ステップ５）。ここで、二次元ウェーブレット変換は、帯域分割フィルタとダウンサンプラとを、適宜組み合わせれば実現できる。

なお、ここでは変換係数ＬＬを使用しない。これは、変換係数ＬＬを使用すると、画質劣化が顕著になるためである。また、画像の輪郭付近では、変換係数ＨＬ、ＬＨ、ＨＨの値が大きく、変換係数ＨＬ、ＬＨ、ＨＨを操作することにより、電子透かしを輪郭付近に集中して埋め込むことができる。

【００４９】

次に、透かし埋め込み部８は、ステップ６～ステップ１０の処理において、注目する変換係数Ｗを取り出し、埋め込みビット列による処理を施し、施した後の変換係数Ｗ’を求めてゆく。即ち、ステップ６にて、変換係数Ｗが零ならば、変

換係数Ｗをそのまま変換係数Ｗ’とし、次の変換係数Ｗへ注目を移す（ステップ１０）。

【００５０】

一方、変換係数Ｗが零でなければ、埋め込みビット列の注目ビット値を参照する（ステップ７）。このビット値が１ならば、Ｗ＞０のときＷ’＝Ｗ＋β、Ｗ＜０のときＷ’＝Ｗ－βとする（ステップ８）。また、このビット値が０ならば、Ｗ＞０のときＷ’＝Ｗ－β、Ｗ＜０のときＷ’＝Ｗ＋βとする（ステップ９）。そして、全ての変換係数Ｗについて、以上の処理を繰り返す（ステップ１０）。

【００５１】

ここで、値βは、８β＜α（⇔β＜α／８）なる条件を満たす正の整数である。これは、次の理由による。ステップ３により、画素の振幅値をα倍したことにより、生の署名画像がｎ階調とすると、振幅値のとりうる値は、

ｉα　　（ｉ＝０，１，２，…，ｎ－１）

である。

これをウェーブレット変換すると、変換係数ＨＬ、ＬＨ、ＨＨのとりうる値は、

±ｉα／４　（ｉ＝０，１，２，…，４（ｎ－１））

である。

【００５２】

つまり、変換係数同士の間隔の最小値は、α／４であり、これら変換係数同士の中点までの距離はα／８である。したがって、上記条件（β＜α／８）を満たせば、ステップ８，９の加減算を行っても、加減算後の変換係数は、この中点よりも、元の変換係数側にあることになり、加減算後の変換係数と元の変換係数とを取り違えるおそれがなくなる。逆に言えば、この条件に従っている限り、付加情報の埋め込み／取り出しが、自在に、しかも可逆的に、行えるのである。例えば、β＝１とするときには、αを９以上の整数に選べば良い。

【００５３】

次に、全ての変換係数Ｗに対する処理がすんだら、透かし埋め込み部８は、ステップ１１にて、逆二次元ウェーブレット変換を行い、埋め込み済み署名画像を得て、これを出力する（ステップ１２）。この逆二次元ウェーブレット変換は、

帯域合成フィルタとアップサンプラなどを適宜組み合わせれば、実現できる。

【００５４】

次に、図４を用いて、透かし取り出し部１０の動作を説明する。まず、透かし取り出し部１０は、制御部１が埋め込み済み用紙データベース９から取り出した、埋め込み済み署名画像を入力する（ステップ２０）。次に、埋め込み済みビット列を記憶する領域を初期化し（ステップ２１）、埋め込み済み署名画像を二次元ウェーブレット変換して（ステップ２２）、変換係数ＨＬ、ＬＨ、ＨＨを取得する（ステップ２３）。

【００５５】

次に、透かし取り出し部１０は、ステップ２４～ステップ２９の処理によって、埋め込みビット列を取り出すと共に、埋め込み前の、生の署名画像を再生する。なお、生の署名画像の再生は、省略しても良い。即ち、ステップ２４にて、注目する変換係数W’を取り出し、この変換係数W’が零ならば、変換係数W’をそのまま変換係数Wとし、次の変換係数W’に注目を移す（ステップ２９）。

【００５６】

一方、変換係数W’が零でなければ、ステップ２５に移る。ステップ２５では、まず、変換係数W’の絶対値Ａを求め、絶対値Ａのα／４による商Ｋを求める。そして、次の距離Ｌ（＝Ａ－Ｋα／４）と距離Ｒ（＝（Ｋ＋１）α／４－Ａ）とを求めて大小比較する。この距離Ｒは、絶対値Ａから右側（大きい方）の±ｉα／４までの距離であり、距離Ｌは、絶対値Ａから左側（小さい方）の±ｉα／４までの距離である。

【００５７】

ここで、上述したように、$\beta < \alpha / 8$なる条件を満たしているから、変換係数Wを±βだけずらした、変換係数W’は、隣接しうる変換係数W±α／４よりも、元の変換係数Wに近いという関係がある。したがって、Ｌ＜Ｒなるときは、絶対値Ａに対する、元の変換係数Wの絶対値は、必ず絶対値Ａに近い側（左側、小さい方）にあり、図２のステップ８の処理が行われている。逆に、Ｒ＜Ｌなるときは、図２のステップ９の処理が行われている。

【００５８】

このため、Ｌ＜Ｒなるとき、ステップ２７にて、注目する埋め込みビット値を１とし、図２のステップ８の逆変換を行って、元の変換係数Ｗを得る。一方、Ｒ＜Ｌなるときは、ステップ２８にて、注目するビット値を０とし、図２のステップ９の逆変換を行って、元の変換係数Ｗを得る。因みに、８β＜αなる条件を満たす限り、Ｒ＝Ｌとなることはない。勿論、ステップ２５の処理は、一例に過ぎず、変換係数Ｗ’から正しく元の変換係数Ｗを求めることができれば、他の処理で代用しても差し支えない。

【００５９】

以上の処理（ステップ２４～ステップ２９）を繰り返せば、埋め込みビット列を可逆的に取り出すことができ、元の変換係数ＨＬ、ＬＨ、ＨＨ（生の署名画像に係る）の全てを再生できる。そして、透かし取り出し部１０は、この埋め込みビット列を出力する（ステップ３０）。また、透かし取り出し部１０は、元の変換係数を逆二次元ウェーブレット変換し（ステップ３１）、全画素の振幅値を１／α倍して元に戻し（ステップ３２）、再生した生の署名画像を出力する（ステップ３３）。

【００６０】

次に、図５を参照しながら、本形態の電子署名装置の全体動作を説明する。まず、ステップ４０にて、制御部１は、表示部２にログオン可能表示をさせ、署名者のＩＤ、パスワードなどの入力を求める。入力があると、制御部１は、署名権があるかどうかをＩＤ等を用いて、チェックし、署名権の確認がとれた場合のみ、次に進むことを許す（ステップ２４）。

【００６１】

次に、制御部１は、用紙マスタデータベース６を参照して、表示部２に使用可能な用紙のリストを表示させ、署名者に使用したい用紙を選択させる（ステップ４２）。用紙が決まると、制御部１は、埋め込み情報付与部７に指示して、この用紙にユニークな埋め込みビット列を生成させる（ステップ４３）。そして、署名者に署名を行うかどうか糺す（ステップ４４）。署名しないのであれば、制御部１は、処理を継続するかどうか尋ね（ステップ５０）、継続するならステップ４２へ戻り、継続しないなら終了する。

【００６２】

ステップ４４にて、署名者が署名を行う旨、入力部３から指示すると、制御部１は、署名画像データベース５を検索して、この署名者に関連する署名画像を表示部２にリスト表示させる。また、署名者は、リスト以外からも、例えばファイル名を指定するなどして、署名画像を指定できる（ステップ４５）。

【００６３】

署名画像が指定されると、制御部１は、指定された署名画像に完全に一致する画像が、署名画像データベース５に存在するかどうかチェックする（ステップ４６）。もし、署名画像データベース５に存在しない署名画像が指定されていると、これは不正転用されたものである可能性がある。そこで、この場合、制御部１は、指定された署名画像を、透かし取り出し部１０に渡し、図４のフローチャートに沿って、埋め込みビット列を取り出させる（ステップ５１）。

【００６４】

そして、制御部１は、取り出した埋め込みビット列が、ステップ４３で生成したビット列と一致するかどうかチェックする（ステップ５２）。もし、一致しなければ、制御部１は、指定された署名画像は不正転用されたものとして、不正判断を行い（ステップ４３）、署名を拒否し、以後の入力を拒絶する。一方、ステップ５２で一致を見れば、制御部１は、署名画像は正当として、ステップ４８へ移る。

【００６５】

ここで、ステップ５２において、一致となるのは、同じ用紙に同じ署名画像を複数使うような場合である。即ち、一つの署名が正当に行われた後、この署名画像をコピー＆ペーストして、同じ用紙の他の箇所へ用いると、一致となる。このようなときは、最初の署名時に正当性をチェックしてあるから、署名画像の同一用紙内の転用を認めても、差し支えない。

【００６６】

さて、ステップ４６にて、署名画像データベース５に完全に一致する画像が見つかると、制御部１は、生の署名画像が正当に指定されたものと判断し、透かし埋め込み部８へ指示して、図２のフローチャートに沿って、埋め込みビット列を

電子透かしとして埋め込ませ、埋め込み済み署名画像を得る（ステップ４７）。そして、制御部１は、埋め込み済み署名画像を用紙の所定領域に貼り付けた画像を生成して、表示部２を介して署名者に提示すると共に、この画像を埋め込み済み用紙データベース９に保存させる（ステップ４８、４９）。そして、制御部１は、以上の処理を、継続が希望されるだけ（ステップ５０）、繰り返す。

【００６７】

以上の説明により、単一人の署名だけでなく、各人が次々に署名を行えることが容易に理解されよう。

【００６８】

次に、図６～図１０を用いて、本形態の電子署名装置による署名例を説明する。まず図６～図９は、用紙の例として、稟議書を示している。図６に示すように、この稟議書は、右上部に「起案者」、「課長」、「部長」、「本部長」、「社長」のそれぞれが、署名（この例では捺印）すべき、矩形の捺印欄が設けてあり、図示した状態では、既に、「起案者」（山口）、「課長」（田中）が捺印を済ませ、「部長」が捺印したばかりのところである。そして、「部長」は、鈴木某であり、彼の生の署名画像を拡大すると、図７のようになる。

【００６９】

また、ここでは、「１９９９０７２６１０３２９７８６３」という、付加情報が設定され、これをビット展開したビット列が、埋め込みビット列とされる。因みに、「１９９９０７２６１０３２」なる数字は、１９９９年７月２６日１０時３２分という、用紙作成時間であり、「９７８６３」なる数字は、この稟議書の識別子である。勿論、これは一例に過ぎず、付加情報は種々設定できるし、図示しているように、付加情報を表示する必要はないことは、いうまでもない。

【００７０】

さて、図７の生の署名画像に対して、上記ビット列を埋め込む電子透かし（図２のフローチャートに準拠）だけを取り出して図示すると、図８のようになる。図７と図８とを比べれば、この電子透かしは、輪郭付近に集中していることは、明らかであろう。このようにすると、人間の視覚特性から、２値画像またはそれに近い、署名画像であっても、極めて知覚されにくい、電子透かしを埋め込むこ

とができる。その証拠に、埋め込み済み署名画像を図９に示しているが、図７と図９とを目視で比較しても、その差異を見つけることは、ほとんど不可能である。因みに、図６の捺印欄には、埋め込み済み署名画像（「部長」の捺印欄には、図７ではなく図９の画像）が表示される。

【００７１】

また、この例では、捺印を取り扱ったが、署名画像を包囲する領域（図６では、捺印欄）の形状やサイズを適宜変更すれば、図１０に示すような、サインを用いる場合や、指紋などにも、本発明は、同様に適用できる。さらには、捺印、サイン、指紋などが混在する状態で使用される場合にも、同様に対応できる。

【００７２】

ここで、本明細書にいう「電子署名プログラムをコンピュータ読み取り可能に記録した記録媒体」には、複数の記録媒体にプログラムを分散して配布する場合を含む。また、このプログラムが、オペレーティングシステムの一部であるか否かを問わず、種々のプロセスないしスレッド（ＤＬＬ、ＯＣＸ、ＡｃｔｉｖｅＸ等（マイクロソフト社の商標を含む））に機能の一部を肩代わりさせている場合には、肩代わりさせた機能に係る部分が、記録媒体に格納されていない場合も含む。

【００７３】

図１には、スタンドアロン形式のシステムを例示したが、サーバー／クライアント形式にしても良い。つまり、１つの端末機のみに、本明細書に出現する全ての要素が含まれている場合の他、１つの端末機がクライアントであり、これが接続可能なサーバないしネットワーク上に、全部又は一部の要素が実存していても、差し支えない。

【００７４】

さらには、図１のほとんどの要素をサーバー側で持ち、クライアント側では、例えば、ＷＷＷブラウザだけにしても良い。この場合、各種の情報は、通常サーバ上にあり、基本的にネットワークを経由してクライアントに配布されるものだが、必要な情報が、サーバ上にあるときは、そのサーバの記憶装置が、ここにいう「記録媒体」となり、クライアント上にあるときは、そのクライアントの記録

装置が、ここにいう「記録媒体」となる。

【００７５】

さらに、この「電子署名プログラム」には、コンパイルされて機械語になったアプリケーションの他、上述のプロセスないしスレッドにより解釈される中間コードとして実存する場合や、少なくともリソースとソースコードとが「記録媒体」上に格納され、これらから機械語のアプリケーションを生成できるコンパイラ及びリンカが「記録媒体」にある場合や、少なくともリソースとソースコードとが「記録媒体」上に格納され、これらから中間コードのアプリケーションを生成できるインタープリタが「記録媒体」にある場合なども含む。

【００７６】

【発明の効果】

請求項１、１０、１９では、用紙固有の電子透かしを用いて、署名画像の不正転用を防止できる。

【００７７】

請求項２、１１、２０では、極めて知覚されにくい電子透かしとすることができ、従前の慣習に近く、違和感が少ない、環境を提供できる。

【００７８】

請求項３、１２、２１では、用紙全体のイメージを、簡単に取り出せる。

【００７９】

請求項４、１３では、知覚されにくい電子透かしを、周波数領域に分けて埋め込める。

【００８０】

請求項５、１４、２２では、２値画像又はそれに近い低階調の署名画像に対し、より知覚されにくい電子透かしを埋め込める。

【００８１】

請求項６、１５、２３では、十分なセキュリティと、処理速度とを両立できる。

【００８２】

請求項７、１６、２４では、取り出した付加情報を利用して、不正を抑制でき

る。

【００８３】

請求項８、１７、２５では、不正署名をシステム上で排除できる。

【００８４】

請求項９、１８、２６では、様々な署名画像に対応できる。

【図面の簡単な説明】

【図１】

本発明の一実施の形態における電子署名装置のブロック図

【図２】

同透かし埋め込み部のフローチャート

【図３】

同変換係数の説明図

【図４】

同透かし取り出し部のフローチャート

【図５】

同電子署名装置のフローチャート

【図６】

同捺印を用いる用紙の例示図

【図７】

同生の署名画像の拡大図

【図８】

同電子透かしの拡大図

【図９】

同埋め込み済み署名画像の拡大図

【図１０】

同サインを用いる用紙の例示図

【符号の説明】

１　制御部

２　表示部

３　入力部

４　署名画像入力部

５　署名画像データベース

６　用紙マスタデータベース

７　埋め込み情報付与部

８　透かし埋め込み部

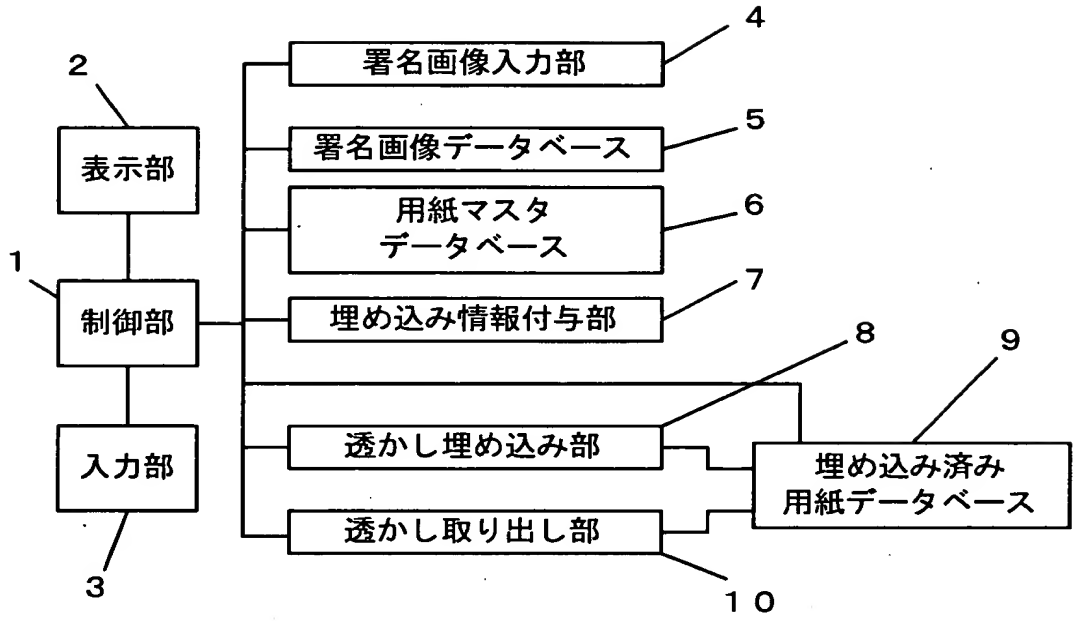
９　埋め込み済み用紙データベース

１０　透かし取り出し部

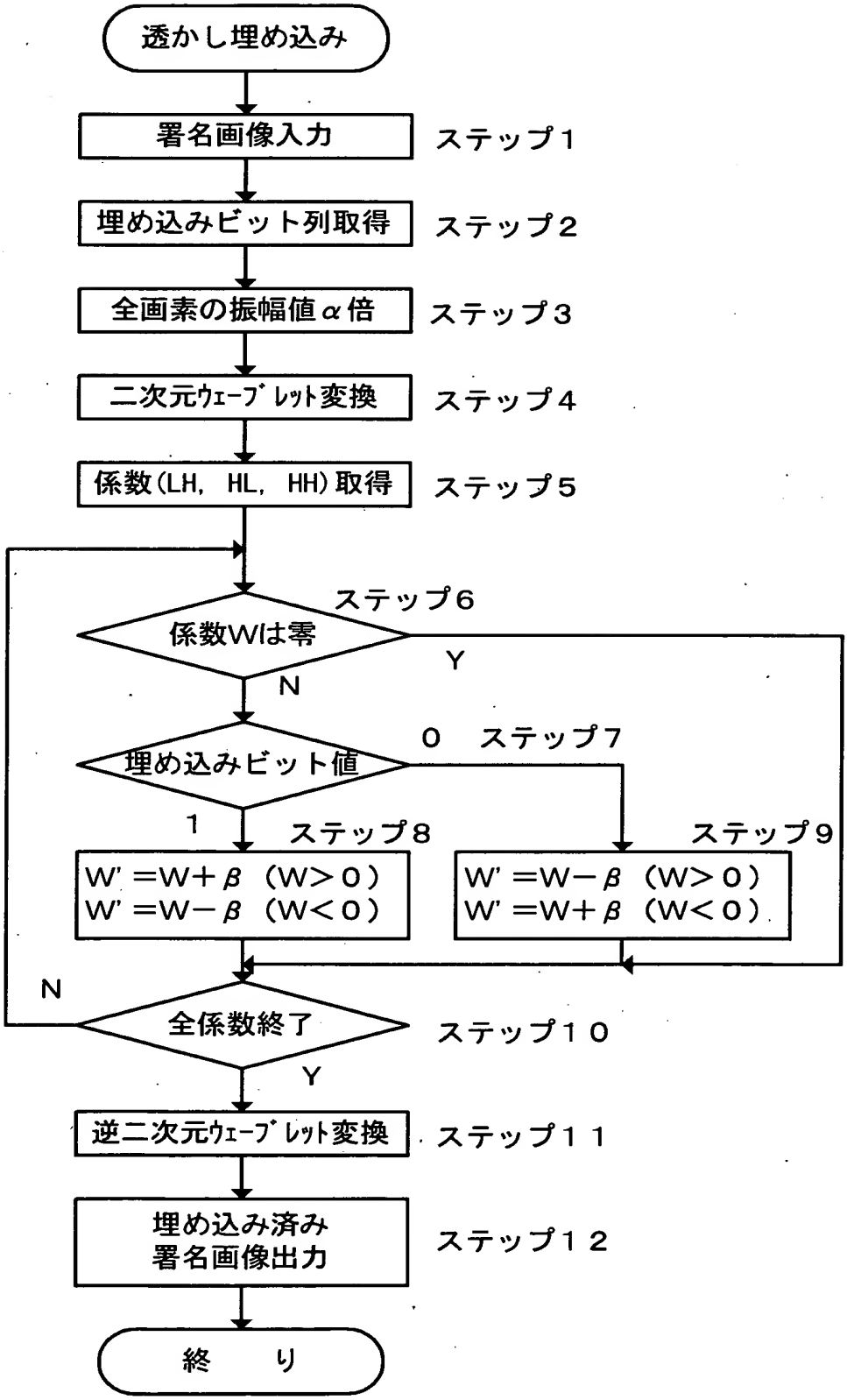
ＨＬ、ＬＨ、ＨＨ　変換係数

【書類名】　図面

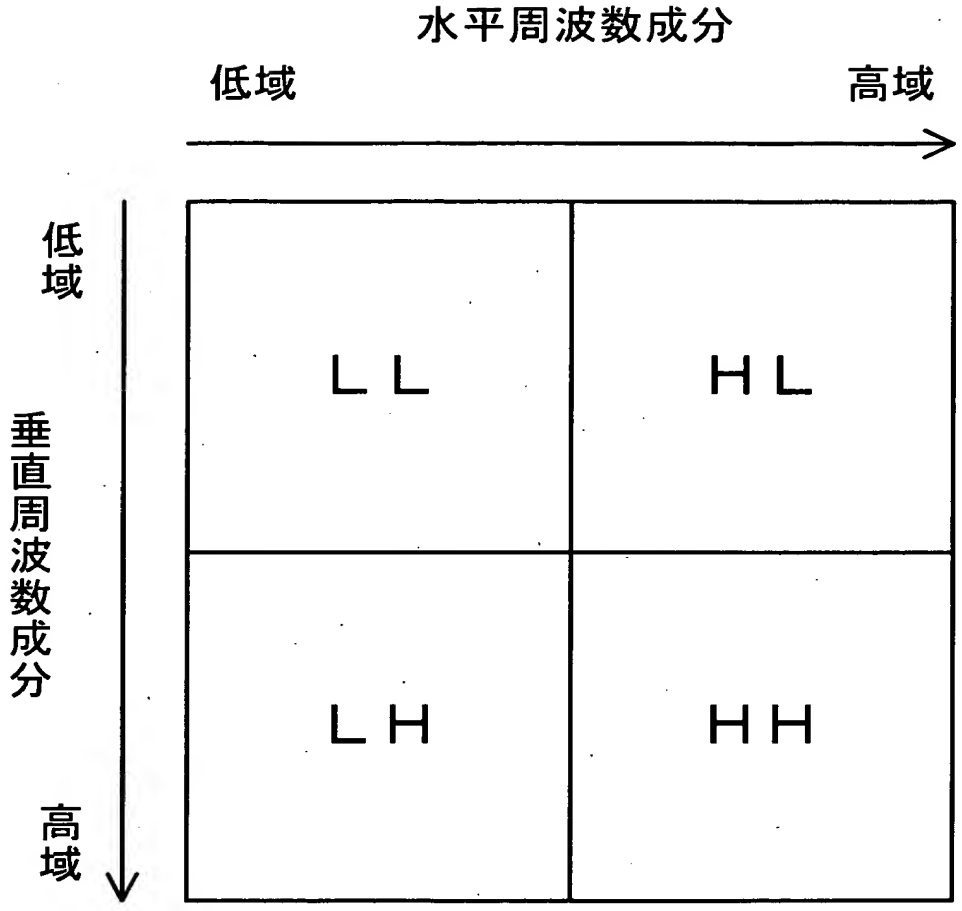
【図１】


2
表示部
1
制御部
入力部
3
署名画像入力部
4
署名画像データベース
5
用紙マスタ
データベース
6
埋め込み情報付与部
7
8
透かし埋め込み部
9
埋め込み済み
用紙データベース
透かし取り出し部
１０

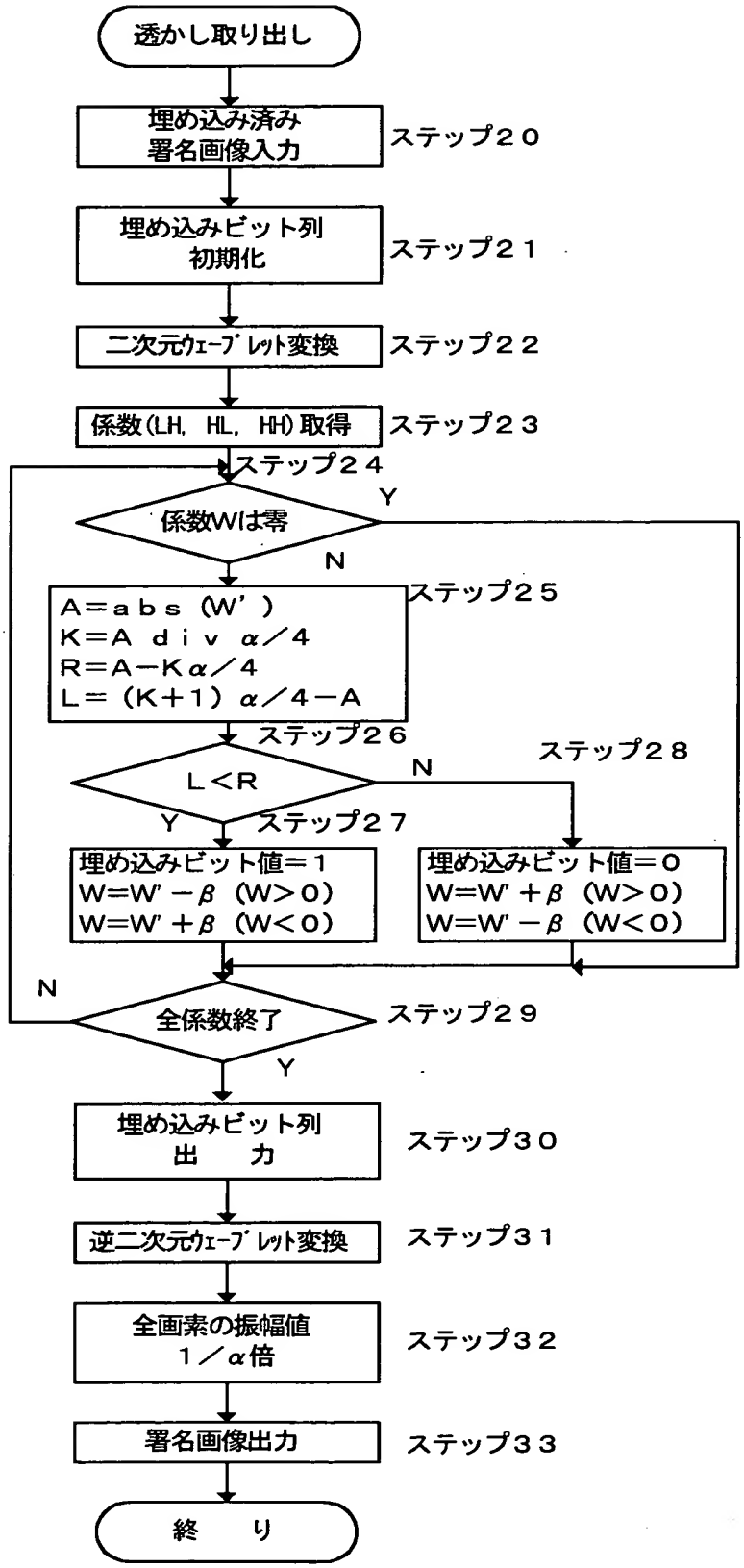
【図２】


透かし埋め込み
署名画像入力
ステップ１
埋め込みビット列取得
ステップ２
全画素の振幅値α倍
ステップ３
二次元ｳｪｰﾌﾞﾚｯﾄ変換
ステップ４
係数(LH，HL，HH)取得
ステップ５
ステップ６
係数Wは零
Y
N
埋め込みビット値
０　ステップ７
１
ステップ８
W'＝W＋β（W＞０）
W'＝W－β（W＜０）
ステップ９
W'＝W－β（W＞０）
W'＝W＋β（W＜０）
N
全係数終了
ステップ１０
Y
逆二次元ｳｪｰﾌﾞﾚｯﾄ変換
ステップ１１
埋め込み済み
署名画像出力
ステップ１２
終　り

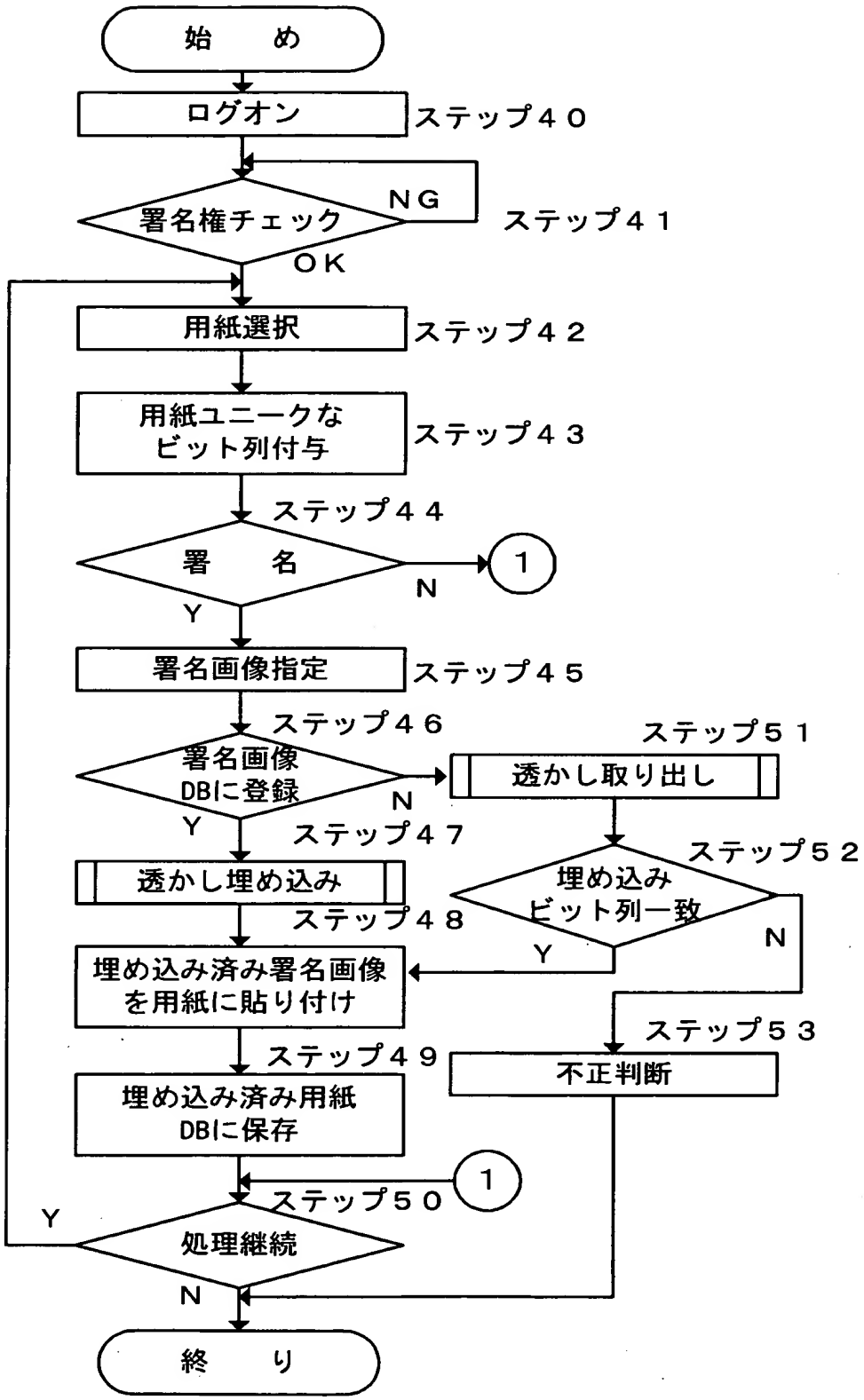
【図３】



【図４】


透かし取り出し
埋め込み済み
署名画像入力
ステップ２０
埋め込みビット列
初期化
ステップ２１
二次元ウェーブレット変換
ステップ２２
係数(LH, HL, HH)取得
ステップ２３
ステップ２４
係数Wは零
Y
N
A＝ａｂｓ（W'）
K＝A ｄｉｖ α／４
R＝A－Kα／４
L＝（K＋１）α／４－A
ステップ２５
ステップ２６
L＜R
N
Y
ステップ２７
ステップ２８
埋め込みビット値＝１
W=W'－β（W＞０）
W=W'＋β（W＜０）
埋め込みビット値＝０
W=W'＋β（W＞０）
W=W'－β（W＜０）
N
全係数終了
ステップ２９
Y
埋め込みビット列
出　力
ステップ３０
逆二次元ウェーブレット変換
ステップ３１
全画素の振幅値
１／α倍
ステップ３２
署名画像出力
ステップ３３
終　り

【図５】


始　め
ログオン
ステップ４０
署名権チェック
NG
ステップ４１
OK
用紙選択
ステップ４２
用紙ユニークな
ビット列付与
ステップ４３
ステップ４４
署　名
N
1
Y
署名画像指定
ステップ４５
ステップ４６
署名画像
DBに登録
N
ステップ５１
透かし取り出し
Y
ステップ４７
透かし埋め込み
ステップ５２
埋め込み
ビット列一致
N
ステップ４８
Y
埋め込み済み署名画像
を用紙に貼り付け
ステップ５３
不正判断
ステップ４９
埋め込み済み用紙
DBに保存
1
ステップ５０
Y
処理継続
N
終　り

【図６】

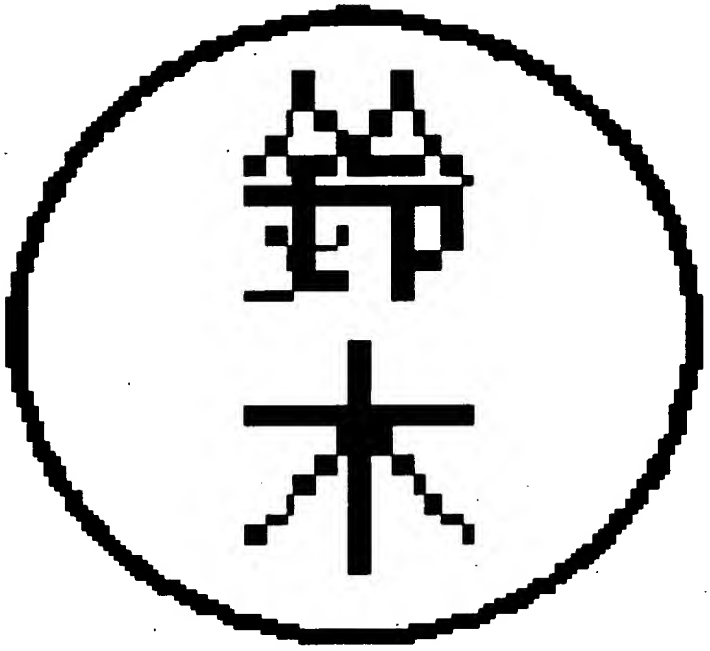
<1990726103297863>

稟議書

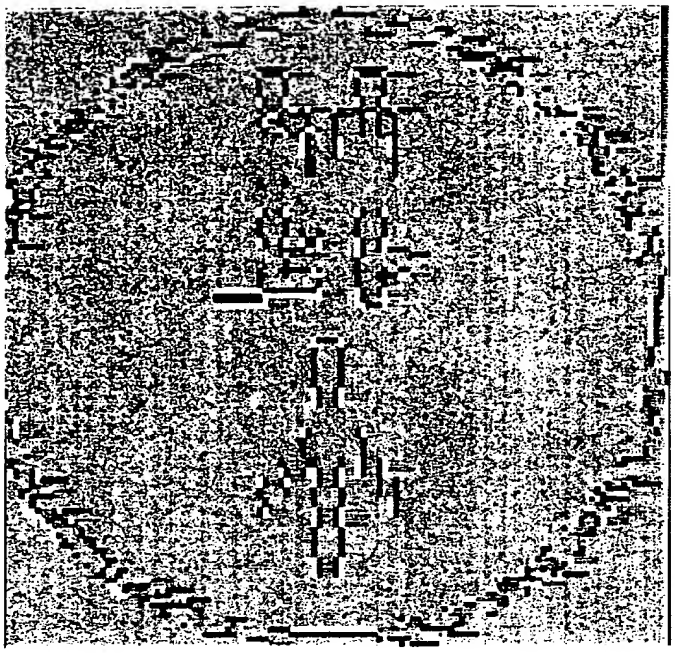
社　長	本部長	部　長	課　長	起案者
		鈴木	田中	山口

件名		文書番号	稟第１２３４号
		起 案 日	1999年 7月26日
		決 裁 日	年　月　日

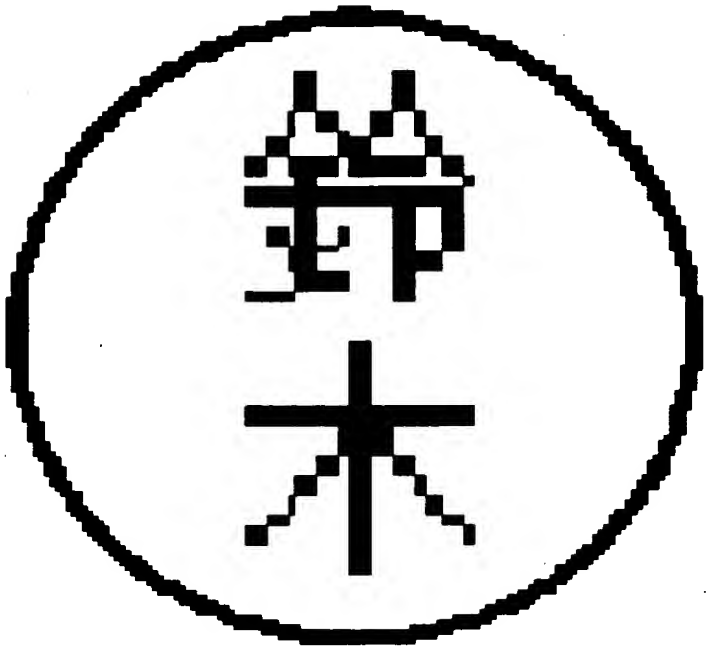
【図７】



【図８】



【図９】



【図１０】

Signature: Taro Matsushita

Date : July 26, 1999

<1990726103297864>

【書類名】　要約書

【要約】

【課題】　従来の慣習に近く、署名の性質に合った電子署名装置を提供する。

【解決手段】　署名画像入力部４から生の署名画像を入力する。入力された生の署名画像に、透かし埋め込み部８が電子透かしを埋め込み、埋め込み済み用紙データベース９に、電子透かしが埋め込まれた署名画像を蓄積する。透かし埋め込み部は、用紙毎にユニークな付加情報を、署名画像の輪郭付近に集中して埋め込む。２値画像に近い署名画像においても、電子透かしは、極めて知覚されにくく、しかも、署名画像の不正転用を防止できる。

【選択図】　図３

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社